

宣言定数の抽象化による形式的部品の再利用性向上

原野和貴[†]

電気通信大学情報理工学域 I 類

織田健[‡]

電気通信大学大学院情報学専攻

1 はじめに

近年、ソフトウェアの複雑化により、開発コストの増大や信頼性の低下が問題となっている。それに対し、部品再利用や形式手法の研究がなされている。部品再利用に基づくソフトウェア自動合成は要求仕様を分解して捉え、個々の要求仕様を満たす部品を検索で得て結合を行う。そこで、形式手法の B メソッドで書かれたモデルと実装の組を部品とするソフトウェア自動合成手法が提案され [1]、要求モデルと部品のモデルの等価性を判定し部品が再利用される。しかし、従来手法では定数値の不一致で再利用性が低下する問題が存在する。本研究では、スカラー値の宣言定数に対し置換を行い再利用性を向上させる手法を提案する。

2 研究背景

2.1 部品再利用に基づくソフトウェア自動合成

ソフトウェア自動合成とは、仕様記述にある要求を満たすプログラムを自動的に作り出す技術である [2]。部品再利用に基づく自動合成の考え方はユーザの要求仕様を単純な要求仕様の集まりに分解して捉え、個々の要求仕様を満たす部品を検索で取得し、後でこれらを組み合わせるものである [1]。

2.2 B メソッド

B メソッドは数学的基盤に基づく形式手法の 1 つで、仕様記述からコード生成までを支援する [3]。これは仕様に対応するモデルから実装への段階的詳細化に基づき、各段階の無矛盾性と詳細化の整合性を機械的に検証する。B メソッドにおける定数は識別子を与え宣言される定数とコード内に直接存在する数値がある。宣言された定数は詳細化の任意の段階で必ず定数値が与えられ、定数値を制限する制約条件を持つ。スカラー値の宣言定数の制約条件は必ず型宣言を持ち、上限や下限の制約や他の宣言定数との関係を示す制約などを持つ。加えて、モデルで宣言された定数は既に等価演算子の制約条件によって値が与えられていても実装の中で必ず値が与えられる。

2.3 モデル充足ソフトウェア合成手法

モデル充足ソフトウェア合成 (MSSS) 手法は B メソッドで記述された既存ソフトウェアから生成されるモデルと実装の組を部品とするソフトウェア自動合成手法である [1]。この手法では、要求モデルと部品のモデルの等価性を文字列一致により判定することで要求モデルを満たす部品の再利用を行なっている。また、要求モデルや部品の元である既存ソフトウェアのモデルには事前に同

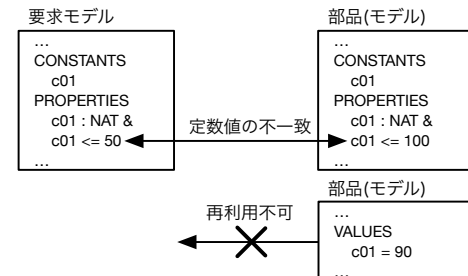


図 1: 定数値の不一致による再利用性低下

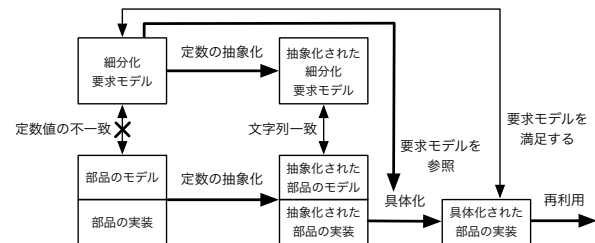


図 2: 置換による再利用性向上の概念図

様の手法で推論などによる文字列の統一と操作分割や分割された操作の制約条件の抽出による細分化を行う。

3 課題と解決方針

3.1 定数値の不一致による形式的部品の再利用性低下

MSSS 手法では文字列一致によるモデルの等価性判定を行い、厳密に等価なモデルをもつ部品のみを再利用している。図 1 の例では文字列の統一と細分化がなされた要求モデルと部品のモデルにおいて、省略箇所の文字列は一致しており CONSTANTS 節で宣言される定数 c01 における PROPERTIES 節の制約条件内の数値が異なっている。これらのモデルは等価でなく部品は再利用されない。しかし、この部品は定数値を変更することで再利用できる可能性があり、部品の再利用性が低下している。

3.2 課題解決の方針

前節の課題に対して、モデルの宣言定数を抽象化することでモデル同士を一致させ再利用性の向上を図る。抽象化した定数は部品の結合後に要求モデルに合った値を与え具体化を行い要求モデルを満足させる (図 2 左)。

4 宣言定数の置換による再利用性向上

本章では、宣言定数の置換により再利用性を向上させる手法の説明を行う。また、従来の MSSS 手法では本手法を適用できないためその解決法を説明する。

4.1 宣言定数の置換

提案手法ではモデル細分化後に宣言定数を抽象化する手順を加え、要求モデルと部品に同様の抽象化を行い定数値の差が吸収された等価性判定を行う。そして、検索で得られた部品の実装の結合後に要求モデルに合わせて

An Improving Reusability of Formal Components by Abstracting Declared Constants

[†]Kazuki Harano, The University of Electro-Communications

[‡]Takeshi Oda, The University of Electro-Communications, Graduate School of Information and Communication Engineering

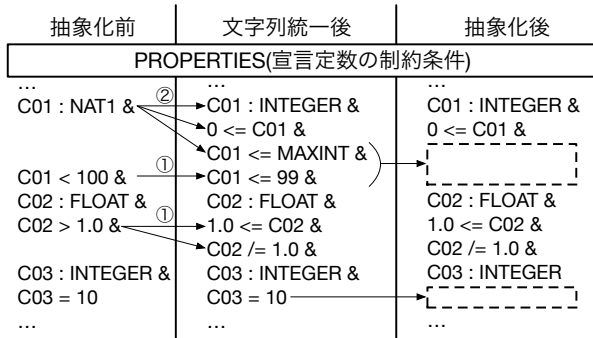


図 3: 表記の統一と抽象化の例

定数値を与え具体化する。また、実装での宣言定数の具体化に対応し事前に部品の実装に抽象化を行う。以下にそれぞれの手順を説明する。

4.1.1 モデルでの宣言定数の抽象化

モデルでの抽象化では、宣言定数の数値を含む制約条件の表記を統一させ、後述する特定の制約条件を削除する。また、これは要求モデルと部品に同様の手法を適用するが、要求モデルでは部品の結合後の具体化で参照する制約条件であるため保管しておく。

宣言定数の制約条件の表記の統一

削除対象となる制約条件の種類の削減や等価判定時の文字列の統一のために、制約条件を削除する前に宣言定数の制約条件の表記の統一を行う。

主な操作は演算子と型宣言の表記を統一する(図3右)。1つ目の演算子の統一では、大小比較の演算子を1つ('<=')にまとめる(場合により、'/='も含む)。2つ目の型宣言の表記の統一では型の所属述語において、複数の種類の型を最も原始的な型へ統一する。

削除対象とする宣言定数の制約条件

抽象化において削除の対象とする宣言定数の制約条件は「1つの宣言定数と数値のみで構成される比較('<=')または等値('=')の制約条件」である(図3)。

しかし、2つ以上の宣言定数で構成される制約条件は宣言定数間の関係を示し、たとえ数値が含まれていても無矛盾性の保証のため削除しない。また、数値のみで構成される式が0や1など宣言定数の型を制約する数値のときは削除しない。しかし、MAXINTなどの型を実装可能な範囲へ制約する数値の場合は再利用性向上のため削除する。もし上記の削除しない数値を含む制約条件が複数存在しそれらが論理積により省略可能であれば、それらの制約条件はまとめる。

4.1.2 実装での宣言定数の抽象化

実装での宣言定数の抽象化では、部品生成で得られた実装に対して、そのモデルで宣言された定数を抽象化する。その操作は、モデルと対応する定数への代入文の数値を統一の記号('?')に置換する。このとき、実装で初めて宣言された定数の場合は置換しない。

4.1.3 宣言定数の具体化

宣言定数の具体化では、検索で得られた実装を結合した合成実装に対して値を決定し記号を置換して具体化す

る。値の決定では宣言定数の抽象化で削除された制約条件と抽象化後の要求モデルの宣言定数の制約条件を元に決定する。この時、等値演算子の制約条件が存在する場合はその制約条件で記述された数値を用い、存在しない場合は元の制約条件による範囲で取り得る値を用いる。

4.2 宣言定数の置換を考慮したモデル細分化手法

上記の提案手法は宣言定数の制約条件が記述された節の中で削除することで抽象化を行う。しかし、従来のモデル細分化の文字列の統一では宣言定数と変数の制約条件の推論の中で定数値を推移律により変数の制約条件内に直接書くことでモデルの宣言定数の情報を分散している。そのため、モデルの特定の節内に宣言定数の制約条件が登場せず、提案手法を適用できない。

この課題の解決法として、宣言定数と変数の間で推論を行わずそれぞれの節で行い、操作や変数の制約条件の中で使われる宣言定数の制約条件を段階的に抽出することで宣言定数の制約条件を特定の節にまとめたままモデル細分化を行う。

5 評価実験

提案した宣言定数の置換による部品の再利用性向上手法の評価実験として、宣言定数を異なる制約条件で記述した実験用の要求モデルと既存ソフトウェアを用いてソフトウェア合成実験を行なった。要求モデルは8つの細分化モデルへ分割し、既存ソフトウェアから計15の部品を生成し、部品のモデルが要求モデルと一致する部品から合成実装を部品結合により合成した。得られた合成実装は要求モデルを満たすことが証明できた。

6 考察

実験用ソフトウェアより、異なる定数値を持つ要求モデルと部品のモデルからそれらの差を吸収した上で等価性を判定し部品を再利用することができ、再利用性が向上した。また、本手法の健全性は単一の変数を制約する使用法や算術演算での使用などモデルでの単純な記法において確認できたが、全称記号や存在記号など複雑な命題による制約条件を用いた実験により本手法の健全性の確認が必要である。また、本手法はスカラー値の宣言定数が対象だが、コード内に直接書かれる数値の不一致や集合の要素数や列挙集合など定数に関する部品の再利用性低下など解決すべき課題が存在する。

7 終わりに

本研究では、スカラー値の宣言定数を置換することで再利用性を向上させる手法を提案した。今後は、本手法のさらなる健全性の検証と前章で述べた課題の解決による部品の再利用性のさらなる向上を図る必要がある。

参考文献

- [1] 中村 文洋. B Method における部品再利用によるソフトウェア合成と高信頼ソフトウェア部品の整備. 電気通信大学 電気通信学研究科 博士(工学) 学位論文
- [2] 小宮 誠一, 原田 実. 部品合成による自動プログラミング. 情報処理 Vol.28, No. 10. 1987.
- [3] 来間 啓伸. B メソッドにおける形式仕様記述. 近代科学社, 2007